



E-Authentication Interface Specifications for the SAML Artifact Profile

11/3/2003

Draft version 0.1.0



Document History

| Status | Release | Date | Comment | Audience |
|---------------|----------------|-------------|--------------------------------|-----------------|
| Draft | 0.1.0 | 11/03/03 | Initial Draft for distribution | Limited |

Editors

Dave Silver

Terry McBride

Chris Louden

Table Of Contents

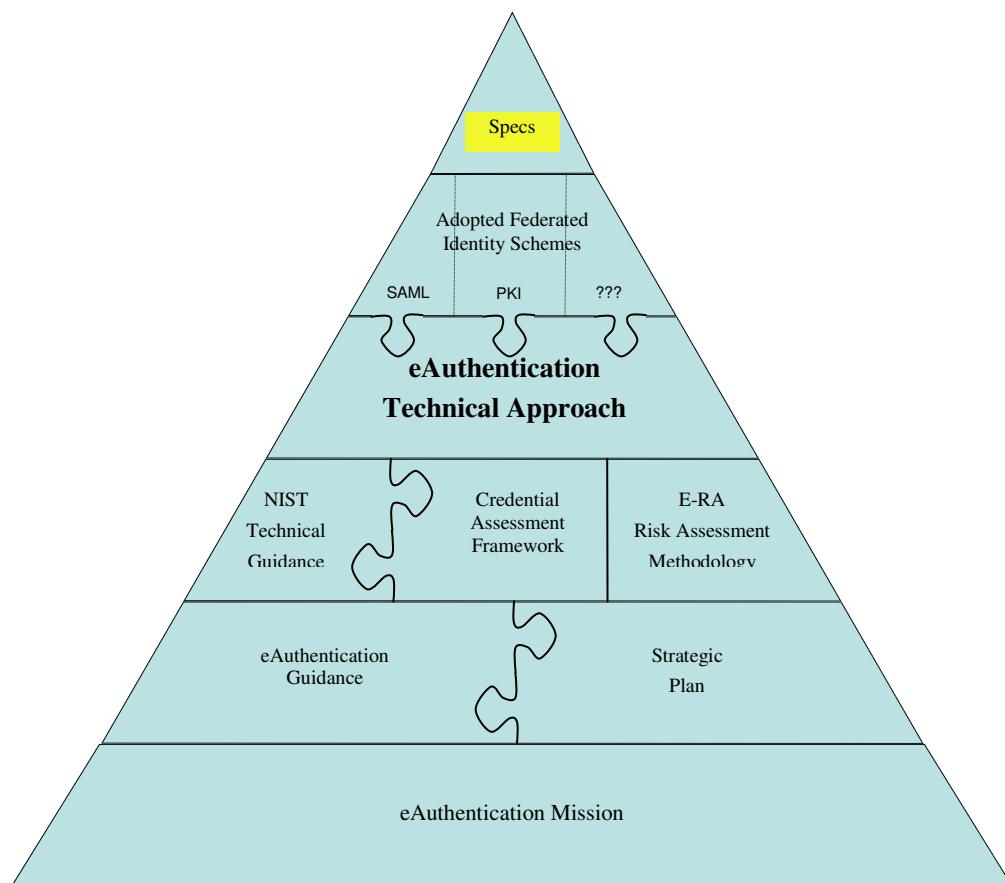
| | | |
|----------|---|----------|
| 1 | INTRODUCTION..... | 1 |
| 1.1 | TERMS..... | 2 |
| 1.2 | DOCUMENT REFERENCES | 3 |
| 1.3 | REFERENCE LINKS | 3 |
| 1.4 | GENERAL APPROACH..... | 1 |
| 2 | CS INTERFACE SPECIFICATION..... | 2 |
| 2.1 | HAND-OFF FROM PORTAL | 2 |
| 2.2 | SINGLE SIGN-ON | 2 |
| 2.3 | TESTING | 2 |
| 3 | AA INTERFACE SPECIFICATION..... | 3 |
| 3.1 | HAND-OFF FROM CS..... | 3 |
| 3.2 | TESTING | 3 |
| 4 | CONFIGURATION METADATA..... | 4 |
| 5 | RULES FOR THE SAML ASSERTION | 5 |
| 6 | APPENDIX A – EXAMPLES | 6 |
| 6.1 | SAMPLE SOAP-WRAPPED SAML ARTIFACT | 6 |
| 6.2 | SAMPLE SOAP-WRAPPED SAML ASSERTION | 7 |
| 6.3 | SAMPLE CONFIGURATION METADATA..... | 9 |

1 INTRODUCTION

This document provides the interface specifications for the SAML Artifact Profile for use with the eAuthentication initiative. The SAML Artifact profile is one of the adopted schemes within the eAuthentication architectural framework.

This document is part of a suite of documents for the eAuthentication initiative. The figure below shows where this document fits into the overall documentation suite. For more information please refer to the eAuthentication Technical Approach. Current versions of these documents are available on the eAuthentication website at <http://www.cio.gov/eAuthentication/>.

Specifications for Agency Applications and Credential Services are both included in this document.



1.1 Terms

This document relies on terminology defined in the NIST E-Authentication Technical Guidance and the OMB Guidance for E-Authentication. The following terms have special meaning in this context:

| Term | Definition |
|--------------------------------------|--|
| Agency Application (AA) | An online service provided by a government agency that requires a user to be authenticated. |
| Assurance Level | Level of trust, as defined by the OMB Guidance for E-Authentication. |
| Claimant | A party whose identity is to be verified using an authentication protocol. |
| Credential | Digital documents used in authentication and access control that bind an identity or an attribute to a claimant's token or some other property such as his or her current network address. Note that this guidance distinguishes between credentials, and tokens (see below) while other documents may lump tokens with credentials. |
| Credential Service (CS) | A service of an Electronic Credential Provider (ECP) that provides credentials to subscribers for use in electronic transactions. If a ECP offers more than one type of credential then each one is considered a separate CS. |
| Electronic Credential Provider (ECP) | An organization that offers one or more Credential Services (CSs). |
| Project Management Office (PMO) | The PMO is the organization that handles E_Authentication program management, administration, and operations for the initiative. |
| Token | Something that the claimant possesses or knows (typically a key or password) that can be used to remotely authenticate the claimant's identity. Technically, the token includes a userid and password that ensures token uniqueness within a credential domain. |

1.2 Document References

- [1] "Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)", OASIS Standard, 5 November 2002. Oasis-sstc-saml-bindings-1.0.
- [2] "Assertions and Protocol for the OASIS Security Markup Language (SAML)", OASIS Standard, 5 November 2002. Oasis-sstc-saml-core-1.0.
- [3] "Simple Object Access Protocol (SOAP) 1.1", W3C, W3C Note 08 May 2000, NOTE-SOAP-20000508.
- [4] "RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile", Internet RFC/STD/FYI/BCP Archives).
- [5] "Liberty Metadata Description and Discovery Specification", Version 1.0-10, Liberty Alliance Project.

1.3 Reference Links

| Topic | Link |
|----------|--|
| SAML | http://www.w3.org http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security http://www.oasis-open.org/committees/security/docs |
| SOAP | http://schemas.xmlsoap.org/soap/envelope http://schemas.xmlsoap.org/soap/encoding |
| XML | http://www.w3.org/1999/XMLSchema-instance http://www.w3.org/1999/XMLSchema |
| X.509 | http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1779.html#sec-2.3 http://www.faqs.org/rfcs/rfc2459.html |
| Metadata | http://www.projectliberty.org/specs/draft-lib-arch-metadata-v1.0-10.pdf http://lists.oasis-open.org/archives/security-services/200304/msg00169.html |

1.4 General Approach

This interface specification is based upon SAML 1.0, and provides guidance on how to use SAML 1.0 specifically for eAuthentication purposes. The specification does not revise or extend SAML 1.0. Where this specification does not explicitly provide SAML guidance, the eAuthentication participant must implement to SAML 1.0 requirements.

The SAML browser Artifact Profile must be used. For details regarding SAML Artifact, see “Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)”, section 4.

Authentication between the SAML Requester and the SAML Responder must be implemented by the following methods, as described in “Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)”, section 3.1.3.2, items 2 and 4:

- HTTP over SSL 3.0 or TLS 1.0 client authentication with a client-side certificate¹

The eAuthentication initiative will issue the client and server certificates.

All CSs and AAs will be issued identifiers by the PMO. These identifiers are referred to as <CSid> and <AAid> respectively. The identifiers are used as keys to reference metadata such as inter-site transfer URLs for each component and will be made available for download by all CSs and AAs. See section 4 for more information on metadata.

¹ In rare cases the PMO may allow password based authentication on a case by case basis.

2 CS INTERFACE SPECIFICATION

2.1 Hand-off From Portal

The user will be redirected from the portal to the CS with an <AAid> in the query string. If the <AAid> is not included in the query string then the user has not selected their AA from the portal, so they must be redirected to the application selection service at the portal with the CS identifier included on the query string:

```
http://eauth.firstgov.gov/service/select?csid=<CSid>
```

If an <AAid> is passed, the CS must authenticate the user, then initiate a hand-off to the AA via the SAML Artifact profile. For details regarding SAML Artifact, see “Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)”, section 4.1.1. See section 5 for further specification of the assertion. Authentication of the user is done according to the methods assessed by the eAuthentication PMO for approval as an eAuthentication CS.

Authentication between the SAML Requester and the SAML Responder must be implemented by the following methods, as described in “Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)”, section 3.1.3.2, items 2 and 4:

- HTTP over SSL 3.0 or TLS 1.0 client authentication with a client-side certificate

The eAuthentication initiative will issue the client and server certificates.

2.2 Single Sign-on

Seamless single sign-on must be supported. When the Portal hands-off to the CS a user who is already authenticated, the CS must immediately hand-off the user to the AA without user interaction. The CS may allow individual users to opt-out of this feature, or require a user to opt-in, but the feature must be supported. The duration of the authentication session is at the discretion of the CS, subject to the methods assessed by the eAuthentication PMO for approval as an eAuthentication CS.

2.3 Testing

The CS must support test processing in the production environment. The ECP must implement several test accounts within their system. Each test account must be assigned an assurance level = Test. All test accounts and passwords must be made available to the eAuthentication PMO, and should not be modifiable using test credentials.

3 AA INTERFACE SPECIFICATION

3.1 Hand-off From CS

The user is passed to the AA from the CS. If the user attempts to access the AA directly they should be redirected to the portal CS selection service with <AAid> included on the query string:

`http://eauth.firstgov.gov/service/select?aaid=<AAid>`

The user is handed off from the CS using the SAML Artifact Profile. For details, see “Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)”, section 4. See section 5 for further specification of the assertion.

Authentication between the SAML Requester and the SAML Responder must be implemented by the following methods, as described in “Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)”, section 3.1.3.2, items 2 and 4:

- HTTP over SSL 3.0 or TLS 1.0 client authentication with a client-side certificate

The eAuthentication initiative will issue the client and server certificates.

If the hand-off fails, the AA must redirect the user to the eGov Portal via:

`http://eAuth.firstgov.gov/errors/handoff/samlart?aaid=<AAid>`

If the AssuranceLevel attribute in the Assertion has a value less than is required by the AA, the AA must display a page indicating that the assurance level is insufficient for the user to access the application and include a link that transfers the user to the eGov Portal:

`http://eAuth.firstgov.gov/help/level?csid=<CSid>&aaid=<AAid>`

3.2 Testing

The AA must support test processing in the production environment. The AA must inspect the AssuranceLevel attribute in the Assertion for an AssuranceLevel = “Test”. If found, the AA must display a page to the user indicating the test was successful. The page should include the <commonName> attribute from the assertion, the name of the CS, and the name of the AA. The test user should not be granted access to any protected resources.

The page must also contain the following status text:

`test with <commonName> from <CSid> to <AAid> <status>`

where <status> contains either “successful” or “failed”

The status text may be hidden from the user.

4 CONFIGURATION METADATA

SAML interoperability requires partners to have some information about other sites, including:

- Location of the Soap Responders
- Issuer attribute
- AssuranceLevel attribute

Metadata is managed by the PMO. It will be available to eAuthentication partners via download from the Portal. The metadata is expressed according to the “Liberty Metadata Description and Discovery Specification”.

Both the CS and the AA must download eAuthentication configuration metadata, and auto-configure their SAML services accordingly.

For a configuration metadata example, see Appendix A of this document.

5 RULES FOR THE SAML ASSERTION

1. The <Assertion> Issuer attribute is assigned by the E_Authentication initiative.
2. The <NameIdentifier> element must be provided within the <AuthenticationStatement> complex type.
3. The <NameIdentifier> value must be in X.509v3 SubjectName format. See “RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile”.
4. The set of name=value pairs must contain a uid element such that no two subscribers within a credential service can share the same uid.
5. The <AttributeStatement> must exist and contain the following <Attribute> and respective <AttributeValue> elements:
 - a. CommonName (e.g., “John H. William Smith III”)
 - i. Must contain surname and given name if known. Otherwise, must contain the user’s pseudonym or userid.
 - b. AssuranceLevel (e.g., “2”)
 - i. Must be one of the following valid values: 1, 2, 3, 4, or Test.
 - ii. Other than the personal information explicitly cited in this specification, Assertions must not contain any other personal information.

6 APPENDIX A – EXAMPLES

6.1 Sample SOAP-Wrapped SAML Artifact

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/1999/XMLSchema-instance"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/1999/XMLSchema"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
    <SOAP-ENV:Body>
        <samlp:Request
            xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
            MinorVersion="0" MajorVersion="1" RequestID="3234487234324"
            xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
            IssueInstant="2003-10-22T16:35:40Z">
            <samlp:AssertionArtifact>AAHJwitt2KE3M/msiV5vz4QwxqVRlcZNX0AP3mPtROrMmic
5+DVJCzAx</samlp:AssertionArtifact>
        </samlp:Request>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

6.2 Sample SOAP-Wrapped SAML Assertion

```
soap-env:Envelope
xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
<soap-env:Body>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
ResponseID="UCIwfB7OKt0L1ChV4JGuf7Ke/so=" InResponseTo="3234487234324"
MajorVersion="1" MinorVersion="0" IssueInstant="2003-10-22T17:19:19Z"
Recipient="192.168.2.104">
<samlp:Status>
<samlp:StatusCode Value="samlp:Success">
</samlp:StatusCode>
</samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
MajorVersion="1" MinorVersion="0"
AssertionID="Tnw9QeaqJFn3lmCjK+eRdTGAkmI=01"
Issuer="crichton.testlab.enspier.com:58080"
IssueInstant="2003-10-22T17:19:17Z" >
<saml:Conditions NotBefore="2003-10-22T17:14:17Z"
NotOnOrAfter="2003-10-22T17:21:17Z" >
</saml:Conditions>
<saml:AuthenticationStatement
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"
AuthenticationInstant="2003-10-22T17:19:14Z">
<saml:Subject>
<saml:NameIdentifier
NameQualifier="dc=enspier,dc=com">uid=michael,ou=People,o=Website,dc=enspier
,dc=com</saml:NameIdentifier>
<saml:SubjectConfirmation>
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:artifact-01</saml:Co
nfirmationMethod>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:SubjectLocality IPAddress="151.196.49.222"
/></saml:AuthenticationStatement>
<saml:AttributeStatement >
<saml:Subject>
<saml:NameIdentifier
NameQualifier="dc=enspier,dc=com">uid=michael,ou=People,o=Website,dc=enspier
,dc=com</saml:NameIdentifier>
<saml:SubjectConfirmation>
```

```
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:artifact-01</saml:Co  
nfirmationMethod>  
</saml:SubjectConfirmation>  
</saml:Subject>  
<saml:Attribute AttributeName="AssuranceLevel"  
AttributeNamespace="crichton">  
<saml:AttributeValue  
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">4</saml:AttributeValue>  
</saml:Attribute>  
<saml:Attribute AttributeName="commonName" AttributeNamespace="crichton">  
<saml:AttributeValue  
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">Michael  
Crichton</saml:AttributeValue>  
</saml:Attribute>  
</saml:AttributeStatement>  
</saml:Assertion>  
</samlp:Response>  
</soap-env:Body>  
</soap-env:Envelope>
```

6.3 Sample Configuration Metadata

```
<?xml version="1.0" encoding="UTF-8"?>
<EntitiesDescriptor validUntil="2003-11-19T16:12:23Z"
xmlns="urn:liberty:metadata:2003-08"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <!-- CSs -->
    <EntityDescriptor providerID="http://cs.bofa.com" >

        <SingleSignOnServiceURL>https://cs.bofa.com:9985/saml_responder</SingleS
ignOnServiceURL>

        <SingleSignOnProtocolProfile>http://projectliberty.org/profiles/brws-
art</SingleSignOnProtocolProfile>
            <Extension>
                <eAuth:AssuranceLevel
xmlns:eAuth="urn:fed:gov:eAuth:metadata:2003-11">3</AssuranceLevel>
            </Extension>
        </IDPDescriptor>
        <Organization>
            <OrganizationName>Bank of Atlantis</OrganizationName>
            <OrganizationDisplayName>B of A</OrganizationDisplayName>

            <OrganizationUrl>http://www.bankofatlantis.com</OrganizationUrl>
            </Organization>
            <ContactPerson>
                <ContactType>technical</ContactType>
                <Company>Bank of Atlantis</Company>
                <GivenName>John</GivenName>
                <SurName>Smith</SurName>
                <EmailAddress>john@bankofatlantis.net</EmailAddress>
                <TelephoneNumber>555.555.5555</TelephoneNumber>
            </ContactPerson>
        </EntityDescriptor>
        <EntityDescriptor providerID="http://www.roseandlefty.net" >

            <SingleSignOnServiceURL>https://www.roseandlefty.net/saml/ObSAMLResponde
rService</SingleSignOnServiceURL>

            <SingleSignOnProtocolProfile>http://projectliberty.org/profiles/brws-
art</SingleSignOnProtocolProfile>
                <Extension>
                    <eAuth:AssuranceLevel
xmlns:eAuth="urn:fed:gov:eAuth:metadata:2003-11">1</AssuranceLevel>
                </Extension>
            </IDPDescriptor>
            <Organization>
```

```
<OrganizationName>Rose and Left</OrganizationName>

<OrganizationUrl>http://www.roseandlefty.net</OrganizationUrl>
    </Organization>
</EntityDescriptor>
<!-- AAs -->
<EntityDescriptor>
    <SPDescriptor providerID="http://widget.fed.gov" >
        <AssertionConsumerServiceURL
isDefault="true">https://widget.fed.gov:9985/saml_in</AssertionConsumerService
URL>
            <AuthnRequestsSigned>false</AuthnRequestsSigned>
            <Extension>
                <eAuth:AssuranceLevel
xmlns:eAuth="urn:fed:gov:eAuth:metadata:2003-11">1</AssuranceLevel>
            </Extension>
        </SPDescriptor>
        <Organization>
            <OrganizationName>Department of Widget
Regulation</OrganizationName>
            <OrganizationUrl>http://.widget.fed.gov</OrganizationUrl>
        </Organization>
    </EntityDescriptor>
    <EntityDescriptor>
        <SPDescriptor providerID="http://electronicinfoservice.us.gov" >
            <AssertionConsumerServiceURL
isDefault="true">https://electronicinfoservice.us.gov/saml/ObSAMLReceiverServ
ice</AssertionConsumerServiceURL>
            <AuthnRequestsSigned>false</AuthnRequestsSigned>
            <Extension>
                <eAuth:AssuranceLevel
xmlns:eAuth="urn:fed:gov:eAuth:metadata:2003-11">2</AssuranceLevel>
            </Extension>
        </SPDescriptor>
        <Organization>
            <OrganizationName>Electronic Information
Service</OrganizationName>
            <OrganizationDisplayName>Electronic Information Service
Online Research</OrganizationDisplayName>

            <OrganizationUrl>http://electronicinfoservice.us.gov</OrganizationUrl>
        </Organization>
    </EntityDescriptor>
</EntitiesDescriptor>
```